UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/262,123	03/03/1999	DAVID CARROLL CHALLENER	RP9-98-089	8958

28722 7590 09/13/2004

BRACEWELL & PATTERSON, L.L.P.
P.O. BOX 969
AUSTIN, TX 78767-0969

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 09/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/262,123	03/03/1999	DAVID CARROLL CHALLENER	RP9-98-089	8958

7590 10/16/2002

ANDREW J DILLON
FELSMAN BRADLEY VADEN GUNTER AND DILLON
SUITE 350 LAKEWOOD ON THE PARK
7600B NORTH CAPITAL OF TEXAS HIGHWAY
AUSTIN, TX 78731

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/16/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/262,123	**Applicant(s)** CHALLENER ET AL.	10
	Examiner Kambiz Zand	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 02 October 2002.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-16 are pending.

Response to Arguments

4. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

5. Applicant's arguments with respect to the claim(s) have been considered but are moot in view of the new ground(s) of rejection

Claim Rejections - 35 USC § 102

6. **Claims 1 and 9** are rejected under 35 U.S.C. 102(b) as being anticipated by Micali (5,315,658A).

As per claims 1 and 9 Micali (5,315,658A) teach a method and a system in a data processing system for maintaining multiple secure user private keys in a non-secure storage device, said method and system comprising the steps of: establishing a master key pair for said system, said master key pair including a master private key and a master public key (see col. 11, lines 41-44 wherein government's key pair considers as a Master key pair consist of a public/private key); storing said master key pair in a protected storage device (see col. 11, lines33-37 wherein the Master key pair may be stored within a secure chips); establishing a unique user key pair for each multiple users, each of said a user key pairs including a user private key and a user public key (see col. 11, lines 41-44 and 61-67 wherein each user or employee has his own set of public/private key); encrypting each of said user private keys utilizing said master public key (see col.11, lines 43-44 wherein each user private's key is encrypted with government (Master key) public key and storing each of said encrypted user private keys in said non secure storage device (see col.12, lines 2-5 wherein the storage may be a non-secure storage) wherein each of said encrypted user private keys is secure while stored in said non-secure storage device (see col.11, lines 43-44 and 62-67; col.12, lines 1-4).

Claim Rejections - 35 USC § 103

7. **Claims 1-4 and 9-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A).

As per claims 1 and 9 Boneh et al. (6,134,660) teach a method and a system in a data processing system for maintaining multiple secure user private keys in a non-secure storage device, said method and system comprising the steps of: establishing a master key for said system (see col. 6, lines 38-40), said master key storage generates pair of private keys and public keys (see col. 7, lines 45-47); storing said master key in a protected storage device (see col. 7, lines 55-56; fig. 2); establishing a unique user key pair for each multiple users, each of said a user key pairs including a user private key and a user public key (see col. 8, lines 18-27); encrypting each of said user private keys utilizing said master key; and storing each of said encrypted user private keys in said non secure storage device (see col. 7, lines 50-63; fig. 2), wherein each of said encrypted user private keys is secure while stored in said non-secure storage device (fig. 2, item108) but do not disclose the master key as a public/private Master key. However Matyas et al (5,142,578A) uses the master key as a shared key or session key but in col.9, lines 21-32 refers that the Master key may be replaced by a Master public/private pair for said system, said master key pair including a master private key and a master public key. Therefore it would have been obvious to one of ordinary skilled in the art to utilize Matyas et al (5,142,578A) Master public/private pair in Boneh et al. (6,134,660)'s method and a system such in order to tag and authenticate user's applications processing in a large network setting without compromising application processing security.

As per claims 2 and 10 Boneh et al. (6,134,660) teach the method and the system according to claim 1, further comprising the steps of: establishing an encryption device having an encryption engine and said protected storage device; and said protected storage device being accessible only through said encryption engine (see fig. 3, item 108 through 210).

As per claims 3 and 11 Boneh et al. (6,134,660) teach the method and the system according to claims 2 and 10, further comprising the step of said encryption engine encrypting each of said user private keys utilizing said master public key stored in said protected storage device (see fig. 3, item 204).

As per claims 4 and 12 Boneh et al. (6,134,660) teach the method and the system according to claims 3 and 11, further comprising the steps of: an application generating a message to transmit to a recipient (see fig. 2); said encryption engine decrypting a particular user's private key utilizing said master private key; said encryption engine encrypting said message utilizing said decrypted particular user's private key and a recipient's public key; and said system transmitting said encrypted message to said recipient (see fig. 5B and 6).

Claim Rejections - 35 USC § 103

8. **Claims 5-8 and 13-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A) and further in view of McBride (6,292,899B1).

As per claims 5 and 13 Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A) teach the method and the system according to claims 4 and 12 above, wherein the step of establishing a user key pair as applied to claim 1 above but fail to explicitly point out the step of associating each of said user key pair with an application. However McBride (6,292,899B1) teaches that relationship (see fig. 3, item 301). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to include McBride (6,292,899B1) method with relation to programs and application in Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A) system and method in order to provide secure transmission of programs and application in a wide area network environment.

As per claims 6 and 14 Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A) teach the method and the system as applied to claims 5 and 13 but do not disclose explicitly the steps of: establishing a certificate, said certificate being associated with said application, said particular user's private key, and said user; in response to said user attempting to access said application utilizing said certificate, said encryption engine utilizing said certificate to determine a location within said non secure storage device for said user private key associated with said certificate; said encryption engine decrypting particular said user's private key; and said encryption engine utilizing said decrypted user private key to encrypt messages transmitted by said application. However McBride (6,292,899B1) teaches the above relationship and describes a master file (certificate) associated with the application (see col. 7, lines 7-13; col. 5, lines 40-67). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to include McBride (6,292,899B1) method with relation to use of a master file as a certificate in relation with programs and application in Boneh et al. (6,134,660) in view of Matyas et al (5,142,578A) system and method in order to provide highly secure transmission of programs and application in a wide area network environment.

As per claims 7 and 15 Boneh et al. (6,134,660) teach the method and the system according to claims 1 and 14, wherein said step of storing each of said encrypted user private keys in said non-secure storage further comprises the step of storing each of said encrypted user private keys (see fig. 2-3) but mentions backup tape and not explicitly a hard drive. However it is well known in the art that hard drive are one type of storage device for backing up and storing data. It would have been obvious to one of ordinary skilled in the art to use hard drive as well as other storage medium in order to store different kind of data including backup data.

As per claims 8 and 16 Boneh et al. (6,134,660) teach the method and the system according to claims 7 and 15, further comprising the step of each of said unique user key pairs being capable of being utilized only in said data processing system wherein a particular user key pair is established as applied to claim 1 above wherein said particular user key pair is not capable of being utilized in a second data processing system (see col. 6, lines 65-67; col. 7, lines 1-13).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

After-Final	(703) 746-7238
Official	(703) 746-7239
Non-Official/Draft	(703) 746-7240

Kambiz Zand
K-Z
10/09/02

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100